

ATTACK

在攻与防的对立统一中
寻求技术突破

黑客攻防 从入门到精通

应用大全篇 · 全新升级版

明月工作室 赵玉萍◎编著



附赠
大型视频教程光盘

以下人群请勿翻阅本书:

1. 自以为很牛，对黑客不屑一顾的人
2. 心存侥幸，认为黑客离自己很远的人
3. 习惯黑客攻击，总是折腾他人的人
4. 号太多，习惯被盗号的人
5. 不差钱，不怕被盗刷的人
6. 我不是Boss，对交易安全漠不关心的人

DEFENSE



北京大学出版社
PEKING UNIVERSITY PRESS

黑客攻防

从入门到精通

应用大全篇·全新升级版

明月工作室 赵玉萍◎编著



北京大学出版社
PEKING UNIVERSITY PRESS

内 容 提 要

本书由浅入深、图文并茂地再现了计算机网络安全的多方面知识,包括黑客攻击之前的社会工程学、计算机安全和手机安全方面的知识。

全书共28章,内容为从零开始认识黑客、揭开社会工程学的神秘面纱、社会工程学之信息追踪、用户隐私的泄露与防护、商业信息的安全防护、Windows系统命令行、解析黑客常用的入侵方法、Windows系统漏洞攻防、木马攻防、病毒攻防、后门技术攻防、密码攻防、黑客的基本功——编程、远程控制技术、网站脚本的攻防、黑客入侵检测技术、清除入侵痕迹、局域网攻防、网络代理与追踪技术、系统和数据的备份与恢复、计算机安全防护、网络账号密码的攻防、加强网络支付工具的安全、无线网络黑客攻防、Android操作系统、智能手机操作系统——iOS、智能手机病毒与木马攻防、Wi-Fi安全攻防。

本书语言简洁、流畅,内容丰富全面,既可作为计算机初、中级用户、计算机维护人员、IT从业人员及对黑客攻防与网络安全维护感兴趣的计算机中级用户的教材,也可作为计算机培训班的辅导用书。

图书在版编目(CIP)数据

黑客攻防从入门到精通.应用大全篇:全新升级版/明月工作室,赵玉萍编著.一北京:北京大学出版社,2017.2

ISBN 978-7-301-27902-1

I. ①黑… II. ①明… ②赵… III. ①黑客-网络防御 IV. ①TP393.081

中国版本图书馆CIP数据核字(2016)第314230号

书 名: 黑客攻防从入门到精通(应用大全篇·全新升级版)

HEIKE GONGFANG CONG RUMEN DAO JINGTONG

著作责任者: 明月工作室 赵玉萍 编著

责任编辑: 尹 毅

标准书号: ISBN 978-7-301-27902-1

出版发行: 北京大学出版社

地 址: 北京市海淀区成府路205号 100871

网 址: <http://www.pup.cn> 新浪微博: @北京大学出版社

电子信箱: pup7@pup.cn

电 话: 邮购部62752015 发行部62750672 编辑部62580653

印刷者: 三河市博文印刷有限公司

经 销 者: 新华书店

787毫米×1092毫米 16开本 42.75印张 902千字

2017年2月第1版 2017年2月第1次印刷

印 数: 1-3000册

定 价: 88.00元

未经许可,不得以任何方式复制或抄袭本书之部分或全部内容。

版权所有,侵权必究

举报电话: 010-62752024 电子信箱: fd@puppkuedu.cn

图书如有印装质量问题,请与出版部联系,电话: 010-62756370

前言 · 全新升级版

从2003年起，中国互联网逐渐找到了适合国情的商业模式和发展道路，互联网应用呈现多元化局面，如电子商务、网络游戏、视频网站、社交娱乐等。计算机技术及通信技术的进一步发展，持续催动中国互联网新一轮的高速增长，2008年，中国网民已经达到2.53亿人，首次超过美国，跃居世界首位。

2009年开始，移动互联网兴起；互联网与移动互联网共同营造了当前双网互联的盛世。网络已经成为个人生活与工作中获取信息的重要手段，网络购物也已经成为了民众重要的消费渠道。当前，“互联网+”的战略布局与工业4.0的深度发展，使国家经济发展、民众工作生活，都与网络安全休戚相关，一个安全的网络环境是必不可少的。

当前最大的一个问题是广大用户对网络相关软硬件技术的掌握程度远远不够，这就给不法分子提供了大量的机会，不法分子借助计算机网络滋生的各种网络病毒、木马、流氓软件、间谍软件，给广大网络用户的个人信息及财产安全带来非常大的威胁。

为提升广大用户对于计算机网络安全知识的掌握程度，做好个人信息财产安全的防护，我们出版了这套“黑客攻防从入门到精通”丛书，本书为其中的《黑客攻防从入门到精通（应用大全篇·全新升级版）》分册。

丛书书目

- 黑客攻防从入门到精通（全新升级版）
- 黑客攻防从入门到精通（Web技术实战篇）
- 黑客攻防从入门到精通（Web脚本编程篇·全新升级版）
- 黑客攻防从入门到精通（黑客与反黑工具篇·全新升级版）
- 黑客攻防从入门到精通（加密与解密篇）
- 黑客攻防从入门到精通（手机安全篇·全新升级版）
- 黑客攻防从入门到精通（应用大全篇·全新升级版）
- 黑客攻防从入门到精通（命令实战篇·全新升级版）
- 黑客攻防从入门到精通（社会工程学篇）

■ 本书特点

- 内容全面：本书从计算机安全攻防的社会工程学，到计算机安全攻防入门，再到专业级的Web技术安全知识，适合各个层面、不同基础的读者阅读。此外，对当前移动端应用较多的Wi-Fi、移动支付等新知识进行重点介绍和剖析。
- 与时俱进：本书主要适用于Windows 7及更新版本的操作系统用户阅读。尽管本书中的许多工具、案例等可以在Windows XP等系统下运行或使用，但为了能够顺利学习本书全部的内容，强烈建议广大读者安装Windows 7及更新版本的操作系统。
- 任务驱动：本书理论和实例相结合，在介绍完相关知识点以后，即以案例的形式对该知识点进行介绍，加深读者对该知识点的理解和认知能力，力争彻底掌握该知识点。
- 适合阅读：本书摒弃了大量枯燥文字叙述的编写方式，而采用了图文并茂的方式进行编排，以大量的插图进行讲解，可以让读者的学习过程更加轻松。
- 深入浅出：本书内容从零起步，步步深入，通俗易懂，由浅入深地讲解，使初学者和具有一定基础的用户都能逐步提高。
- 附赠超值光盘：为了读者能全面地了解黑客攻防方面的相关知识，特整理了本书重点部分的黑客攻防全能视频，帮助读者深入学习本书。另外，本书还赠送Windows系统常用快捷键大全、Linux基础命令手册、Linux系统管理与维护命令手册、Linux网络与服务器命令手册、Windows系统安全与维护手册、计算机硬件管理超级手册、Windows文件管理高级手册和黑客攻防操作命令手册等资源。

■ 读者对象

- 计算机初、中级用户。
- 网店店主、网店管理及开发人员。
- 计算机爱好者、提高者。
- 各行各业需要网络防护的人员、中小企业的网络管理员。
- Web前、后端的开发及管理人员。
- 无线网络相关行业的从业人员。
- 计算机及网络相关的培训机构。
- 大中专院校相关学生。

■ 本书结构及内容

全书共23章，内容由浅入深，循序渐进，前后衔接紧密，逻辑性较强。

- 第1章 从零开始认识黑客
- 第2章 揭开社会工程学的神秘面纱
- 第3章 社会工程学之信息追踪
- 第4章 用户隐私的泄露与防护
- 第5章 商业信息的安全防护
- 第6章 Windows系统命令行
- 第7章 解析黑客常用的入侵方法
- 第8章 Windows系统漏洞攻防
- 第9章 木马攻防
- 第10章 病毒攻防
- 第11章 后门技术攻防
- 第12章 密码攻防
- 第13章 黑客的基本功——编程
- 第14章 远程控制技术
- 第15章 网站脚本的攻防
- 第16章 黑客入侵检测技术
- 第17章 清除入侵痕迹
- 第18章 局域网攻防
- 第19章 网络代理与追踪技术
- 第20章 系统和数据的备份与恢复
- 第21章 计算机安全防护
- 第22章 网络账号密码的攻防
- 第23章 加强网络支付工具的安全
- 第24章 无线网络黑客攻防
- 第25章 Android操作系统
- 第26章 智能手机操作系统——iOS
- 第27章 智能手机病毒与木马攻防
- 第28章 Wi-Fi安全攻防



后续服务

本书由赵玉萍编著，胡华、栾铭斌、王栋、宗立波、马琳、闫珊珊、高翔等老师也参加了本书部分内容的编写和统稿工作，在此一并表示感谢！在本书的编写过程中，我们竭尽所能地为您呈现最好、最全的实用功能，但仍难免有疏漏和不妥之处，敬请广大读者不吝指正。

若您在学习过程中产生疑问或有任何建议，可以通过E-mail或QQ群与我们联系。

投稿邮箱：pup7@pup.cn

读者信箱：2751801073@qq.com

读者交流群：218192911（办公之家）、99839857

郑重声明

本书对大量计算机及移动端的攻击行为进行了曝光，方便广大读者针对计算机网络安全做好防范措施。

请广大读者注意：据国家有关法律规定，任何利用黑客技术攻击他人的行为都是违法的！

目录 CONTENTS

第1章 从零开始认识

黑客..... 1

1.1 认识黑客..... 2

1.1.1 区别黑客、红客、蓝客、骇客
及飞客..... 2

1.1.2 认识白帽、灰帽及黑帽黑客..... 2

1.1.3 黑客名人堂..... 3

1.1.4 黑客基础知识..... 3

1.1.5 黑客常用术语..... 4

1.2 常见的网络协议..... 8

1.2.1 TCP/IP 简介..... 8

1.2.2 IP 协议..... 9

1.2.3 地址解析协议 (ARP)..... 11

1.2.4 因特网控制报文协议 (ICMP)..... 12

1.3 了解系统进程..... 13

1.3.1 认识系统进程..... 13

1.3.2 关闭系统进程..... 14

1.3.3 新建系统进程..... 15

1.4 了解端口..... 16

1.4.1 各类端口详解..... 16

1.4.2 查看端口..... 18

1.4.3 开启和关闭端口..... 19

1.4.4 端口的限制..... 21

1.5 在计算机中创建虚拟测试环境..... 27

1.5.1 安装 VMware 虚拟机..... 27

1.5.2 配置安装好的 VMware
虚拟机..... 30

1.5.3 安装虚拟操作系统..... 31

1.5.4 VMware Tools 安装..... 33

技巧与问答..... 34

第2章 揭开社会工程学的神秘面纱..... 36

2.1 社会工程学..... 37

2.1.1 社会工程学概述..... 37

2.1.2 了解社会工程学攻击..... 38

2.1.3 常见社会工程学手段..... 39

2.2 生活中的社会工程学攻击案例..... 40

2.2.1 获取用户的手机号码..... 40

2.2.2 破解密码..... 41

2.2.3 骗取系统口令..... 42

2.3 提高对非传统信息安全的重视..... 43

2.3.1 介绍非传统信息安全..... 43

2.3.2 从个人角度重视非传统信息
安全..... 44

2.3.3 从企业角度重视非传统信息

安全.....	45
技巧与问答.....	47
第3章 社会工程学之信息追踪.....	49
3.1 利用搜索引擎追踪.....	50
3.1.1 百度搜索的深度应用.....	50
3.1.2 了解“人肉”搜索.....	56
3.1.3 企业信息追踪与防护.....	58
3.2 利用门户网站追踪.....	59
3.2.1 认识门户网站.....	60
3.2.2 知名门户网站搜索.....	60
3.2.3 高端门户网站的信息搜索.....	62
3.3 利用综合信息追踪.....	64
3.3.1 找人网.....	64
3.3.2 查询网.....	65
技巧与问答.....	67

第4章 用户隐私的泄露与防护..... 70

4.1 稍不注意就泄密.....	71
4.1.1 网站Cookies.....	71
4.1.2 查看用户浏览过的文件.....	75
4.1.3 用户的复制记录.....	82
4.1.4 软件的备份文件.....	83
4.1.5 软件的生成文件.....	85
4.1.6 查看Windows生成的缩略图.....	86
4.2 来自网络的信息泄露.....	87
4.2.1 隐藏的各种木马和病毒.....	87
4.2.2 认识流氓软件.....	89
4.2.3 很难查杀的间谍软件.....	90

技巧与问答.....	90
------------	----

第5章 商业信息的安全防护..... 93

5.1 盗取目标的相关信息.....	94
5.1.1 翻查垃圾盗取信息.....	94
5.1.2 造假身份盗取信息.....	94
5.1.3 设置陷阱盗取信息.....	95
5.2 概述商业窃密手段.....	96
5.2.1 技术著述或广告展览.....	96
5.2.2 信息调查表格.....	97
5.2.3 手机窃听技术.....	97
5.2.4 智能手机窃密技术.....	98
5.2.5 语音与影像监控技术.....	99
5.2.6 GPS跟踪与定位技术.....	100

技巧与问答.....	102
------------	-----

第6章 Windows 系统命令行..... 103

6.1 全面解读Windows系统中的命令行.....	104
6.1.1 Windows系统中的命令行概述.....	104
6.1.2 Windows系统中的命令行操作.....	108
6.1.3 Windows系统中的命令行启动.....	109
6.2 在Windows系统中执行DOS命令.....	109
6.2.1 通过IE浏览器访问DOS窗口.....	110

6.2.2	用菜单的形式进入DOS窗口	111
6.2.3	复制、粘贴命令行	111
6.2.4	设置窗口风格	113
6.2.5	Windows 系统命令行	115
6.3	黑客常用的Windows 命令行	118
6.3.1	测试物理网络命令 (ping 命令)	118
6.3.2	工作组和域命令 (net 命令)	120
6.3.3	查看网络连接命令 (netstat 命令)	125
6.3.4	23 端口登录命令 (telnet 命令)	128
6.3.5	查看网络配置命令 (ipconfig 命令)	128
6.3.6	传输协议FTP 命令	129
6.4	全面认识DOS 系统	129
6.4.1	DOS 系统的功能	130
6.4.2	文件与目录	131
6.4.3	目录与磁盘	132
6.4.4	文件类型与属性	134
6.4.5	命令分类与命令格式	137
	技巧与问答	138

第7章 解析黑客常用的入侵方法..... 141

7.1	解析网络欺骗入侵	142
7.1.1	网络欺骗的主要技术	142
7.1.2	常见的网络欺骗方式	143
7.1.3	经典案例解析——网络钓鱼	147

7.2	解析缓冲区溢出入侵	150
7.2.1	认识缓冲区溢出	150
7.2.2	缓冲区溢出攻击的基本流程	151
7.2.3	了解缓冲区溢出入侵的方法	151
7.2.4	缓冲区溢出常用的防范措施	153
7.3	解析口令猜解入侵	154
7.3.1	黑客常用的口令猜解攻击方法	154
7.3.2	口令猜解攻击防御	155
7.3.3	口令攻击类型	156
7.3.4	使用SAMInside 破解计算机密码	157
7.3.5	使用LC6 破解计算机密码	159
	技巧与问答	162

第8章 Windows 系统漏洞攻防..... 164

8.1	系统漏洞概述	165
8.1.1	什么是系统漏洞	165
8.1.2	系统漏洞产生的原因	165
8.1.3	常见的系统漏洞类型	166
8.2	RPC 服务远程漏洞的防黑实战	170
8.2.1	RPC 服务远程漏洞	170
8.2.2	RPC 服务远程漏洞入侵演示	171
8.2.3	RPC 服务远程漏洞的防御	172
8.3	Windows 服务器系统入侵	174
8.3.1	入侵Windows 服务器的流程曝光	174

8.3.2	NetBIOS漏洞攻防	176
-------	-------------------	-----

8.4	用MBSA检测系统漏洞, 保护 计算机安全	179
-----	--------------------------------	-----

8.4.1	检测单台计算机	179
-------	---------------	-----

8.4.2	检测多台计算机	181
-------	---------------	-----

8.5	使用Windows Update修复系统 漏洞	181
-----	----------------------------------	-----

技巧与问答	183
-------------	-----

第9章 木马攻防..... 185

9.1	木马概述	186
-----	------------	-----

9.1.1	木马的工作原理	186
-------	---------------	-----

9.1.2	木马的发展演变	186
-------	---------------	-----

9.1.3	木马的组成与分类	187
-------	----------------	-----

9.2	常见的木马伪装方式	189
-----	-----------------	-----

9.2.1	解析木马的伪装方式	189
-------	-----------------	-----

9.2.2	CHM木马	190
-------	-------------	-----

9.2.3	EXE捆绑机	194
-------	--------------	-----

9.2.4	自解压捆绑木马	196
-------	---------------	-----

9.3	加壳与脱壳工具的使用	198
-----	------------------	-----

9.3.1	ASPack加壳工具	199
-------	------------------	-----

9.3.2	NsPack多次加壳工具	200
-------	--------------------	-----

9.3.3	PE-Scan检测加壳工具	201
-------	---------------------	-----

9.3.4	UnASPack脱壳工具	202
-------	--------------------	-----

9.4	木马清除软件的使用	203
-----	-----------------	-----

9.4.1	在“Windows进程管理器”中 管理进程	203
-------	--------------------------------	-----

9.4.2	“木马清道夫”清除木马	205
-------	-------------------	-----

9.4.3	“木马清除专家”清除木马	207
-------	--------------------	-----

技巧与问答	210
-------------	-----

第10章 病毒攻防..... 212

10.1	计算机病毒	213
------	-------------	-----

10.1.1	什么是计算机病毒	213
--------	----------------	-----

10.1.2	计算机病毒的特点	213
--------	----------------	-----

10.1.3	计算机病毒的结构	214
--------	----------------	-----

10.1.4	病毒的工作流程	215
--------	---------------	-----

10.1.5	计算机中病毒后的表现	215
--------	------------------	-----

10.2	VBS脚本病毒	216
------	---------------	-----

10.2.1	VBS脚本病毒的特点	217
--------	------------------	-----

10.2.2	VBS病毒的弱点	217
--------	----------------	-----

10.2.3	常见的VBS脚本病毒 传播方式	218
--------	--------------------------	-----

10.2.4	VBS脚本病毒生成机	219
--------	------------------	-----

10.2.5	如何防范VBS脚本病毒	221
--------	-------------------	-----

10.3	简单病毒	222
------	------------	-----

10.3.1	U盘病毒的生成与防范	222
--------	------------------	-----

10.3.2	Restart病毒制作过程	225
--------	---------------------	-----

10.4	杀毒软件的使用	228
------	---------------	-----

10.4.1	360杀毒软件	228
--------	---------------	-----

10.4.2	用NOD32查杀病毒	230
--------	------------------	-----

技巧与问答	231
-------------	-----

第11章 后门技术攻防 233

11.1	后门基础知识	234
------	--------------	-----

11.1.1	后门的意义及其特点	234
--------	-----------------	-----

11.1.2	后门技术的发展历程	234
--------	-----------------	-----

11.1.3	后门的不同类别	235
--------	---------------	-----

11.2	使用不同工具实现系统服务 后门技术	236
------	----------------------------	-----

11.2.1	Instsrv工具	236
--------	-----------------	-----

11.2.2	Srvinstw 工具	237
11.3	认识账号后门技术	242
11.3.1	手动克隆账号技术	242
11.3.2	软件克隆账号技术	245
11.4	检测系统中的后门程序	246
	技巧与问答	248

第 12 章 密码攻防..... 250

12.1	加密与解密基础	251
12.1.1	加密与解密概述	251
12.1.2	加密的通信模型	251
12.2	常见的各类文件的加密方法	251
12.2.1	在 WPS 中对 Word 文件 进行加密	251
12.2.2	使用 CD-Protector 软件给 光盘加密	252
12.2.3	在 WPS 中对 Excel 文件进行 加密	254
12.2.4	使用 WinRAR 加密压缩 文件	256
12.2.5	使用 Private Pix 软件对多媒体 文件加密	257
12.2.6	宏加密技术	259
12.2.7	NTFS 文件系统加密数据	261
12.3	各类文件的解密方法	262
12.3.1	两种常见 Word 文档解密 方法	262
12.3.2	光盘解密方法	264
12.3.3	Excel 文件解密方法	265
12.3.4	使用 RAR Password Recovery 软件解密压缩文件	266

12.3.5	解密多媒体文件	267
12.3.6	解除宏密码	267
12.3.7	NTFS 文件系统解密数据	268
12.4	操作系统密码攻防方法揭秘	270
12.4.1	密码重置盘破解系统登录 密码	270
12.4.2	Windows 7 PE 破解系统登录 密码	273
12.4.3	SecureIt Pro (系统桌面 超级锁)	277
12.4.4	PC Security (系统全面加密 大师)	279
12.5	文件和文件夹密码的攻防方法 揭秘	282
12.5.1	通过文件分割对文件进行 加密	282
12.5.2	文件夹加密超级大师	288
12.5.3	使用 WinGuard Pro 给应用程序 加密和解密	291
12.6	黑客常用的加密解密工具	292
12.6.1	文本文件专用加密器	292
12.6.2	文件夹加密精灵	294
12.6.3	终极程序加密器	295
	技巧与问答	297

第 13 章 黑客的基本功—— 编程..... 299

13.1	黑客与编程	300
13.1.1	黑客常用的 4 种编程语言	300
13.1.2	黑客与编程密不可分的 关系	301

13.2 进程编程.....	302
13.2.1 进程的基本概念.....	302
13.2.2 进程状态转换.....	302
13.2.3 进程编程.....	303
13.3 线程编程.....	307
13.3.1 线程基本概念.....	307
13.3.2 线程编程.....	308
13.4 文件操作编程.....	311
13.4.1 读写文件编程.....	311
13.4.2 复制、移动和删除文件 编程.....	314
13.5 网络通信编程.....	314
13.5.1 认识网络通信.....	314
13.5.2 Winsock 编程基础.....	317
13.6 注册表编程.....	324
13.6.1 注册表基本术语.....	324
13.6.2 注册表编程.....	324
技巧与问答.....	329

第 14 章 远程控制技术..... 333

14.1 远程控制概述.....	334
14.1.1 远程控制的技术原理.....	334
14.1.2 基于两种协议的远程控制.....	335
14.1.3 远程控制的应用.....	335
14.2 利用任我行软件进行 远程控制.....	336
14.2.1 配置服务端.....	337
14.2.2 通过服务端程序进行远程 控制.....	338
14.3 用 QuickIP 进行多点控制.....	339

14.3.1 安装 QuickIP.....	339
14.3.2 设置 QuickIP 服务器端.....	340
14.3.3 设置 QuickIP 客户端.....	341
14.3.4 实现远程控制.....	342
14.4 用 WinShell 实现远程控制.....	342
14.4.1 配置 WinShell.....	343
14.4.2 实现远程控制.....	344
14.5 远程桌面连接与协助.....	346
14.5.1 Windows 系统的远程桌面 连接.....	346
14.5.2 Windows 系统远程关机.....	350
14.5.3 区别远程桌面与远程协助.....	351
技巧与问答.....	352

第 15 章 网站脚本的 攻防..... 354

15.1 网站脚本入侵与防范.....	355
15.1.1 Web 安全威胁日趋严重的原因.....	355
15.1.2 Web 脚本攻击常见的方式.....	355
15.1.3 Web 服务器常见 8 种 安全漏洞.....	357
15.1.4 脚本漏洞的根源与防范.....	358
15.2 XPath 注入攻击.....	359
15.2.1 什么是 XPath.....	359
15.2.2 保存用户信息的 XML.....	361
15.2.3 实现 XPath 注入的 JAVA 登录验证源代码.....	361
15.3 使用 NBSI 注入工具攻击网站....	362
15.3.1 NBSI 功能概述.....	362

15.3.2 解析使用NBSI实现注入的过程.....	363	16.2.2 基于主机的入侵检测系统的优点.....	385
15.4 使用啊D注入工具攻击网站.....	364	16.3 基于网络的入侵检测系统.....	386
15.4.1 啊D注入工具的功能概述.....	364	16.3.1 包嗅探器和混杂模式.....	386
15.4.2 解析使用啊D批量注入的过程.....	365	16.3.2 包嗅探器的发展.....	387
15.5 SQL注入工具.....	367	16.4 基于漏洞的入侵检测系统.....	387
15.5.1 实现SQL注入攻击的基本条件.....	368	16.4.1 运用流光进行批量主机扫描.....	387
15.5.2 注入攻击的突破口——寻找攻击入口.....	370	16.4.2 运用流光进行指定漏洞扫描.....	391
15.5.3 决定提交变量参数——SQL注入点类型.....	371	16.5 萨客嘶入侵检测系统.....	392
15.5.4 决定注入攻击方式——目标数据库类型.....	371	16.6 Snort入侵检测系统.....	395
15.6 使用Domain注入工具攻击网站.....	373	16.6.1 Snort的系统组成.....	396
15.6.1 Domain功能概述.....	373	16.6.2 Snort的工作过程.....	396
15.6.2 解析使用Domain实现注入的过程.....	374	16.6.3 Snort命令介绍.....	397
15.7 SQL注入攻击的防范.....	377	16.6.4 Snort的工作模式.....	398
技巧与问答.....	379	技巧与问答.....	399
第 16 章 黑客入侵检测技术.....	381	第 17 章 清除入侵痕迹.....	401
16.1 揭秘入侵检测技术.....	382	17.1 黑客留下的“证据”.....	402
16.1.1 入侵检测概述.....	382	17.1.1 产生日志的原因简介.....	402
16.1.2 入侵检测的信息来源.....	382	17.1.2 为什么要清理日志?.....	405
16.2 基于主机的入侵检测系统.....	384	17.2 日志分析工具WebTrends.....	405
16.2.1 基于主机的入侵检测.....	384	17.2.1 创建日志站点.....	405
		17.2.2 生成日志报表.....	409
		17.3 清除历史痕迹常用的方法.....	411
		17.3.1 使用“CCleaner”清理.....	411
		17.3.2 清除网络历史记录.....	414
		17.3.3 使用“Windows优化大师”进行清理.....	417

17.4 清除服务器日志	418
17.4.1 手工删除服务器日志	418
17.4.2 使用批处理清除远程主机日志	420
17.5 常见的Windows日志清理工具	421
17.5.1 elsave 工具	421
17.5.2 ClearLogs 工具	423
技巧与问答	424

第 18 章 局域网攻防 425

18.1 局域网基础知识	426
18.1.1 局域网简介	426
18.1.2 局域网安全隐患	426
18.2 常见的几种局域网攻击类型	428
18.2.1 ARP 欺骗攻击	428
18.2.2 IP 地址欺骗攻击	428
18.3 局域网攻击工具	429
18.3.1 网络剪刀手 Netcut	429
18.3.2 WinArpAttacker 工具	433
18.4 局域网监控工具	435
18.4.1 LanSee 工具	435
18.4.2 网络特工	437
18.4.3 长角牛网络监控机	440
技巧与问答	445

第 19 章 网络代理与追踪技术 447

19.1 常见的代理工具	448
--------------------	-----

19.1.1 “代理猎手”代理工具	448
19.1.2 “SocksCap32”代理工具	453
19.1.3 防范远程跳板代理攻击	455
19.2 常见的黑客追踪工具	457
19.2.1 使用“NeroTrace Pro”进行追踪	457
19.2.2 实战IP追踪技术	459
技巧与问答	460

第 20 章 系统和数据的备份与恢复 461

20.1 备份与还原操作系统	462
20.1.1 使用还原点备份与还原系统	462
20.1.2 使用GHOST备份与还原系统	464
20.2 备份与还原用户数据	469
20.2.1 使用驱动精灵备份与还原驱动程序	469
20.2.2 备份与还原IE浏览器的收藏夹	470
20.2.3 备份和还原QQ聊天记录	473
20.2.4 备份和还原QQ自定义表情	476
20.3 使用恢复工具恢复误删除的数据	479
20.3.1 使用Recuva恢复数据	479
20.3.2 使用FinalData来恢复数据	483
20.3.3 使用FinalRecovery来恢复数据	487
技巧与问答	489

第 21 章 计算机安全

防护 492

21.1 系统安全设置 493

21.1.1 防范更改账户名 493

21.1.2 禁用 Guest (来宾账户) 494

21.1.3 设置账户锁定策略 495

21.1.4 设置离开时快速锁定桌面 497

21.2 预防间谍软件 497

21.2.1 间谍软件防护基本原理 497

21.2.2 利用“360安全卫士”对
计算机进行防护 498

21.2.3 利用“Spy Sweeper”清除间
谍软件 501

21.2.4 利用“Windows Defender”
清除间谍软件 503

21.3 常见的网络安全防护工具 504

21.3.1 利用 AD-Aware 工具预防
间谍程序 504

21.3.2 利用 HijackThis 预防浏览器
绑架 507

21.3.3 诺顿网络安全特警 510

21.4 清除流氓软件 514

21.4.1 清理浏览器插件 514

21.4.2 利用金山清理专家清除
恶意软件 517

21.4.3 流氓软件的防范 518

技巧与问答 521

第 22 章 网络账号密码的

攻防 523

22.1 QQ 账号及密码攻防

常用工具 524

22.1.1 “啊拉 QQ 大盗”的使用和
防范 524

22.1.2 “雨点 QQ 密码查看器”
的使用与防范 526

22.1.3 “QQ Explorer”的使用与
防范 527

22.2 增强 QQ 安全性的方法 528

22.2.1 定期更换密码 528

22.2.2 申请 QQ 密保 529

22.2.3 加密聊天记录 531

22.3 使用密码监听器 531

22.3.1 密码监听器使用方法 531

22.3.2 查找监听者 532

22.3.3 防止网络监听 533

22.4 邮箱账户密码的攻防 533

22.4.1 隐藏邮箱账户 534

22.4.2 追踪伪造邮箱账户发件人 534

22.4.3 电子邮件攻击防范措施 535

技巧与问答 536

第 23 章 加强网络支付

工具的安全 539

23.1 预防黑客入侵网上银行 540

23.1.1 定期修改登录密码 540

23.1.2 使用工行 U 盾 541

23.2 预防黑客入侵支付宝 541

23.2.1 定期修改登录密码 542

23.2.2 设置安全保护问题 543

23.2.3	修改支付密码	544
23.3	预防黑客入侵财付通	546
23.3.1	启用实名认证	546
23.3.2	定期修改登录密码	547
23.3.3	设置二次登录密码	548
23.3.4	定期修改支付密码	549
23.3.5	启用数字证书	549
23.6.6	修改绑定手机	550
	技巧与问答	551

第 24 章 无线网络黑客 攻防..... 554

24.1	无线路由器基本配置	555
24.1.1	了解无线路由器各种端口	555
24.1.2	了解无线路由器的指示灯	555
24.1.3	配置无线路由器参数	556
24.1.4	配置完成重启无线路由器	558
24.1.5	搜索无线信号连接上网	559
24.2	无线路由安全设置	560
24.2.1	修改 Wi-Fi 密码	560
24.2.2	设置 IP 过滤和 MAC 地址列表	560
24.2.3	关闭 SSID 广播	561
24.2.4	禁用 DHCP 功能	562
24.2.5	无线加密	562
	技巧与问答	563

第 25 章 Android 操作 系统..... 565

25.1	解密 Android 系统	566
25.1.1	Android 操作系统的 发展回顾	566
25.1.2	Android 最新版本	567
25.1.3	Android 最新版本新特性	568
25.2	用备份保护数据	569
25.2.1	手动备份	569
25.2.2	利用 91 助手备份	572
25.3	Android 系统获取 Root 权限	576
25.3.1	Root 原理简介	577
25.3.2	获取 Root 权限的利与弊	577
25.3.3	获取 Root 权限的方法	577
25.4	Android 系统刷机	580
25.4.1	Android 系统刷机常识	580
25.4.2	Android 系统刷机教程	581
25.5	Android 平台恶意软件及病毒	583
25.5.1	ROM 内置恶意软件 / 病毒	583
25.5.2	破坏类恶意软件 / 病毒	584
25.5.3	吸费类恶意软件 / 病毒	584
25.5.4	窃取隐私类恶意软件 / 病毒 ...	585
25.5.5	伪装类恶意软件 / 病毒	586
25.5.6	云更新类恶意软件 / 病毒	586
25.5.7	诱骗类恶意软件 / 病毒	587
	技巧与问答	588

第 26 章 智能手机操作 系统——iOS 589

26.1	iOS 操作系统的发展历程	590
26.1.1	iOS 用户界面	594
26.2	从底层剖析 iOS	595